U.S. DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON

| | |
|---|---|
| TENNIELLE COSSEY, KATHLEEN CONNOR and DONALD BRUCE MOUNTJOY, individually and on behalf of all others similarly situated,<br><br>Plaintiffs,<br><br>vs.<br><br>PREMERA BLUE CROSS, a Washington corporation,<br><br>Defendant. | NO.<br><br>**CLASS ACTION COMPLAINT**<br><br>**Demand for Jury Trial** |

## I. INTRODUCTION

1. Every business that collects and stores sensitive information about its customers has a duty to safeguard that information and ensure the data is secure and remains private. That responsibility is most important where a business keeps and stores highly sensitive data such as the Social Security numbers and medical and financial information belonging to its customers.

2. The data collected and stored by health insurance companies are among the most highly sensitive personal and health information. Health insurance companies, in turn, bear the crucial responsibility to protect this data from compromise and theft.

TERRELL MARSHALL DAUDT & WILLIE PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.350.3528
www.tmdwlaw.com

3. The threat of compromise and theft is significant and well known. In the past several years, cyberattacks have occurred across all industries with increasing frequency. In 2014 alone, over one billion personal data records were compromised by cyberattacks.[1] The healthcare and health insurance industries have not been exempt from these attacks. Indeed, the Ponemon Institute, an independent cyber security research institution, has reported that approximately 90% of health care organizations reported that they were the victims of at least one data breach over the past two years.[2] Similarly, a 2014 report by the Identity Theft Resource Center warned that the medical and healthcare industry accounted for 42.5 % of all data breaches in 2014.[3] These trends show no sign of slowing in 2015. Already, on February 4 of this year, Anthem Inc. disclosed that a database containing as many as 80 million customer files was compromised. The risk of cyberattack is known and undeniable; it is imperative that healthcare and health insurance companies assume a corresponding duty to guard against this known risk and thwart preventable attacks.

4. Defendant Premera Blue Cross is one of the largest health insurance companies in the Pacific Northwest. In Washington and Alaska alone, there are nearly 2 million individuals currently insured by Premera Blue Cross. Premera Blue Cross is a major provider to, among others, Amazon.com Inc., Microsoft Corp., and Starbucks Corp. Unsurprisingly, Premera Blue Cross maintains a massive amount of personal and health information on its past and current insureds. It therefore has a duty to take all reasonable measures to protect this information and safeguard it from theft.

5. This lawsuit arises from Defendant's failure to fulfill its legal duty to protect the sensitive information of its customers. On March 17, 2015, Premera Blue Cross acknowledged

---

[1] CNBC, Year of the hack? A billion records compromised in 2014, http://www.cnbc.com/id/102420088# (last visited Mar. 22, 2015).

[2] *See* Ponemon Institute LLC, Fourth Annual Benchmark Study on Patient Privacy & Data Security 2 (Mar. 2014), http://www.ponemon.org/local/upload/file/ID%20ExpertsPatient%20Privacy%20%26%20Data%20Security%20Report%20FINAL1-1.pdf.

[3] Identity Theft Resource Center, Data Breach Reports (Dec. 31, 2014), http://www.idtheftcenter.org/images/breach/DataBreachReports_2014.pdf.

TERRELL MARSHALL DAUDT & WILLIE PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.350.3528
www.tmdwlaw.com

that its systems had been hacked and the personal and health information of approximately 11 million past and current policyholders was compromised. Hackers gained access to, *inter alia*, customer names, addresses, dates of birth, email addresses, telephone numbers, Social Security numbers, member identification numbers, bank account information, and claims information, including personal clinical data. What is worse, the cyber security systems of Premera Blue Cross were breached just weeks after federal auditors explicitly warned Premera that its security systems were inadequate and could be exploited. This theft is the result of Defendant's failure to implement cyber security measures commensurate with the duties it undertook by storing vast quantities of sensitive customer data.

6. Further, and to compound the harm caused to its customers, Premera Blue Cross knew about the breach for over six weeks before it publicly disclosed the incident. Indeed, Premera Blue Cross has acknowledged that it first learned that its system was compromised on January 29, 2015. It did nothing to warn its customers for over six weeks.

7. Premera Blue Cross has yet to fully and accurately inform those affected of the precise scope of the theft or the nature of the risks of identity theft. It is not clear how many customers Premera Blue Cross has thus far notified, but the company estimates that it will not complete the notification process until April 20, 2015. This is unacceptable. In a data breach situation, it is incumbent upon the breached company to provide accurate and complete information to those at risk so they may immediately protect themselves and their families from further harm. Moreover, the Health Insurance Portability and Accountability Act (HIPAA) requires that Premera Blue Cross provide notice without unreasonable delay and no later than 60 days after discovery of a breach. *See* 45 C.F.R. § 164.404. Washington state law requires Premera to provide notice in the most expedient time possible. *See* RCW 19.255.010. United States Senator Patty Murray expressed similar disquiet about Premera's delay in a March 20, 2015 letter to the company, stating that she had "serious concerns regarding the cyberattack on Premera Blue Cross and the failure of the company to make this information public and begin



TERRELL MARSHALL DAUDT & WILLIE PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.350.3528
www.tmdwlaw.com

notifying current and former policy holders for over six weeks. These failures are particularly troubling given the scope of the attack."[4]

8. In short, Defendant breached its duty to protect and safeguard its customers' personal and health information and to take reasonable steps to contain the damage caused where any such information was compromised.

9. Plaintiffs Tennielle Cossey, Kathleen Connor, and Donald Bruce Mountjoy, current Premera Blue Cross customers, therefore bring this action for themselves and on behalf of all persons similarly situated who are or were insureds under a health insurance policy covered, sold, and/or written by Premera Blue Cross or other health insurance plans affiliated with Premera Blue Cross, as described more fully below. Because Defendant failed to safeguard the personal and health information of its customers, it must stand to account before the law.

## II. PARTIES

10. Plaintiff Tennielle Cossey is a citizen of the state of Nevada and resides in Carson City. Ms. Cossey is currently insured under a Premera Blue Cross policy. As set forth in more detail below, Ms. Cossey has suffered harm because her personal and health information was compromised when the cyber security systems of Premera Blue Cross were breached beginning in and around May 2014, and she has spent and will spend time and money safeguarding herself and her family from this fraud.

11. Plaintiff Kathleen Connor is a citizen of the state of Washington and resides in Olympia. Ms. Connor is currently insured under a Premera Blue Cross policy. She has been a policyholder for approximately six years. Ms. Connor's three adult children have also been insured under her Premera Blue Cross policy, and her youngest child is still insured under her Premera policy. As set forth in more detail below, Ms. Connor has suffered harm because her

[4] Letter from Patty Murray, United States Senator, to Jeffrey Roe, President of Premera Blue Cross (Mar. 20, 2015), *available at* http://www.help.senate.gov/newsroom/press/release/?id=7ab95ff6-13d4-4838-b492-b9d4c94e4e37.



TERRELL MARSHALL DAUDT & WILLIE PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.350.3528
www.tmdwlaw.com

personal and health information was compromised when the cyber security systems of Premera Blue Cross were breached beginning in and around May 2014 and she has spent and will spend time and money safeguarding herself and her family from this fraud.

12. Plaintiff Donald Bruce Mountjoy is a citizen of the state of Washington and resides in Olympia. Mr. Mountjoy is currently insured under a Premera Blue Cross policy. He has been a policyholder for approximately six years. As set forth in more detail below, Mr. Mountjoy has suffered harm because his personal and health information was compromised when the cyber security systems of Premera Blue Cross were breached beginning in and around May 2014.

13. Defendant Premera Blue Cross (hereinafter alternately referred to as "Premera" or "Defendant") is a Washington corporation registered with the Washington Secretary of State to do business in Washington. Premera's corporate headquarters are located at 7001 220th Street SW, Mountlake Terrace, Washington, 98043. Premera also maintains operations in Seattle and Spokane, Washington.

14. Premera provides healthcare benefits in Alaska as Premera Blue Cross Blue Shield of Alaska. It has registered with the Alaska Secretary of State to do business in Alaska. Defendant Premera Blue Cross and Premera Blue Cross Blue Shield of Alaska are independent licensees of the Blue Cross Blue Shield Association.

15. Premera is a health insurance provider that offers comprehensive health, life, vision, dental, stop-loss, disability, and workforce wellness services to over 1.8 million current members in Washington and Alaska. Its fiscal year 2013 revenues were $7.6 billion. In Washington and Alaska, Premera maintains a network of over 27,000 healthcare professionals

16. Premera also maintains several affiliates that are not licensees of the Blue Cross Blue Shield Association. These affiliates include LifeWise Health Plan of Oregon; LifeWise Health Plan of Washington; LifeWise Assurance Company; Connexion Insurance Solutions, Inc.; and Vivacity. In total, Premera's affiliates maintain 1.9 million current members in

TERRELL MARSHALL DAUDT & WILLIE PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.350.3528
www.tmdwlaw.com

Washington, Alaska, and Oregon and boast consolidated fiscal year 2013 revenue of $3.36 billion.

17. Premera, Premera Blue Cross Blue Shield of Alaska, and its affiliates are collectively referred to as "Premera" in this Complaint.

## III. JURISDICTION AND VENUE

18. Jurisdiction is proper in this Court pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d), because members of the proposed Plaintiff Class are citizens of states different from Defendant's home state, and the aggregate amount in controversy exceeds in $5,000,000 exclusive of interests and costs.

19. This Court has personal jurisdiction over Premera because Premera is licensed to do business in Washington, regularly conducts business in Washington, and has minimum contacts with Washington.

20. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a) because Premera regularly conducts business and resides in this district, a substantial part of the events or omissions giving rise to these claims occurred in this district, and Premera has caused harm to class members residing in this district.

## IV. FACTUAL BACKGROUND

### A. Premera Collects and Stores Significant Quantities of Customer Data

21. Premera is one the largest health insurance providers in the Pacific Northwest. There are over 6 million current or former Premera insureds in Washington alone.

22. Premera understands that its customers place a premium on privacy. Thus, Premera provides each of its customers with a Notice of Privacy Practices.[5] It also dedicates a section of its website to explain its privacy and data collection policies.[6]

---

[5] *See* Notice of Privacy Practices, *available at* https://www.premera.com/documents/000160.pdf (last visited Mar. 23, 2015).

[6] *See* https://www.premera.com/wa/visitor/privacy-policy/ (last visited Mar. 22, 2015). The privacy section of Premera's website is substantially similar to the printed Notice of Privacy Practices provided to each Premera customer.

TERRELL MARSHALL DAUDT & WILLIE PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.350.3528
www.tmdwlaw.com

23. Premera assures its customers that it is "committed to maintaining the confidentiality of your medical and financial information," including customers' names, Social Security numbers, addresses, telephone number, account number, medical history, and claims information. Premera assures its customers that it has secured its "electronic systems against unauthorized access," and it acknowledges that "[u]nder both the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Gramm-Leach-Bailey Act, Premera Blue Cross must take measures to protect the privacy of your personal information." Further, Premera warrants that it will "protect the privacy of your information even if you no longer maintain coverage through us."

24. Premera's Notice of Privacy Practices explains that it collects most personal and health information directly from its insureds. In addition, Premera states that it may collect information from third parties such as employers, other healthcare providers, and state and federal agencies.

25. Premera further states that it is required by law to "notify [customers] following a breach of . . . unsecured personal information."

26. As these statements make clear, Premera is aware of the importance its customers place on privacy, as well as its duty to safeguard the personal information that its customers supply to it and to promptly notify its customers in the event of a data breach.

**B. The Premera Data Breach**

27. On or about May 5, 2014, hackers infiltrated Premera's Information Technology (IT) system. Over the course of the following eight months, hackers gained access to as many as 11 million records of current and former Premera customers and employees, as well as Blue Cross Blue Shield customers who received medical treatment in Washington or Alaska. For each affected customer, hackers were able to access the customer's name, date of birth, email address, address, telephone number, Social Security number, member identification number, bank account information, and claims information, including clinical data.



TERRELL MARSHALL DAUDT & WILLIE PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.350.3528
www.tmdwlaw.com

28. Hackers operated inside Premera's systems undetected for nearly nine months until January 29, 2015.

29. Although Premera discovered the breach on January 29, 2015, it did not notify its customers or the public until over six weeks later, on March 17, 2015. At that time, Premera disclosed publicly that hackers had breached its cyber security systems and potentially stolen the personal and health information of 11 million current and former customers and employees. Customer records as far back as 2002 were affected by the breach.

30. Premera stated that the breach affected current and former customers of Premera Blue Cross, Premera Blue Cross Blue Shield of Alaska, and Premera's affiliates, including Vivacity, and Connexion Insurance Solutions, Inc. Several days after the breach, LifeWise Health Plan of Oregon announced that 60,000 of its members were compromised by the breach.

31. In addition, Premera acknowledged that the breach affected members of any Blue Cross Blue Shield plan who had received medical treatment in Washington or Alaska. Moreover, Premera stated that "[i]ndividuals who do business with us and provided us with their email address, personal bank account number or social security number are also affected."[7]

32. Upon information and belief, hackers were able to access customers' health information and financial information because Premera did not store such information on separate databases.

33. Premera President Jeffrey Roe issued a statement accompanying the company's public disclosure. In it, he confirmed that attackers "gain[ed] unauthorized access to [Premera's] Information Technology (IT) systems." Mr. Roe's statement further confirmed that the compromised data included "member name, date of birth, email address, address, telephone number, Social Security number, member identification numbers, bank account

[7] Statement of Jeffrey Roe, *available at* http://www.premeraupdate.com/ (last visited Mar. 22, 2015).



TERRELL MARSHALL DAUDT & WILLIE PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.350.3528
www.tmdwlaw.com

information, and claims information, including clinical information." Mr. Roe assured customers that "the security of our members' personal information is a top priority."[8]

34. Mr. Roe did not explain why Premera waited more than six weeks to notify its customers of the security breach. A statement on its website, however, claims that it waited six weeks so that it could "block the attack" and "cleanse" its IT systems.[9] Premera has not explained why it could not block the attack and cleanse its IT system while simultaneously notifying its customers that their data was compromised.

35. Indeed, around the time that Premera learned of the data breach, Anthem Inc. also discovered that its cyber security system was compromised. Anthem Inc. learned of the breach of its systems on January 27, 2015—two days prior to Premera's discovery. Anthem Inc. publicly disclosed the breach on February 4, 2015. The breach at Anthem Inc. affected 80 million customers, many of them Blue Cross Blue Shield customers across the United States.[10]

36. Because the Anthem Inc. data breach affected so many Blue Cross Blue Shield customers, Premera Blue Cross customers reasonably wondered whether they too should be concerned. On February 5, 2015, however, Jim Grazko, president of Premera Blue Cross Blue Shield of Alaska, assured the public that the Anthem breach did not affect Premera customers.[11] Although perhaps true, on February 5, 2015, Premera knew its own systems had been breached and its own customers affected by that breach. Premera said nothing.

37. Perhaps more disturbing, Premera was explicitly warned by the federal government that its cyber security systems were vulnerable before the breach occurred in May 2014. On April 18, 2014, the Office of Personnel Management delivered the results of an audit

---

[8] *Id.*

[9] *See* FAQ, *available at* http://www.premeraupdate.com/faqs/ (last visited Mar. 22, 2015).

[10] *See* Millions of Anthem Customers Targeted in Cyberattack, New York Times, Reed Abelson & Matthew Goldstein, Feb. 5, 2015, *available at* http://www.nytimes.com/2015/02/05/business/hackers-breached-data-of-millions-insurer-says.html?_r=0 (last visited Mar. 22, 2015).

[11] *See* No Signs So Far that Anthem Health Care Data Breach Affects Alaska, Feb. 5, 2015, *available at* http://www.ktuu.com/news/news/no-signs-so-far-that-anthem-health-care-data-breach-affects-alaska/31119336 (last visited Mar. 22, 2015).

TERRELL MARSHALL DAUDT & WILLIE PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.350.3528
www.tmdwlaw.com

it performed on Premera's IT systems. The audit identified ten areas in which Premera's systems were inadequate and vulnerable to attack.[12]

38. Specifically, the audit found that Premera was not timely implementing critical security patches and other software updates. The audit warned, "Failure to promptly install important updates increases the risk that vulnerabilities will not be remediated and sensitive data could be breached."[13]

39. Auditors determined that several of Premera's servers contained applications so old they were no longer supported by the application's vendor and had known security problems.[14]

40. In addition, Premera's servers were insecurely configured, which rendered them more vulnerable to hacking.[15]

41. Three weeks after Premera received this audit, its system was compromised. Premera, of course, would remain ignorant of the security breach for nearly nine months.

42. In its public disclosure on March 17, 2015, Premera stated that it would notify customers of the breach in a letter sent via US mail. Premera estimated that it would not complete this notification process until April 20, 2015.

43. The statement of Mr. Roe was sent to some Premera customers on March 17, 2015. Ms. Connor and Mr. Mountjoy received a copy of Mr. Roe's statement via U.S. mail. Ms. Connor also received letters addressed to two of her children. As of the date of this filing, Ms. Connor's third child has not received mailed notice of the breach.

---

[12] *See* Feds Warned Premera About Security Flaws Before Breach, Seattle Times, Mike Baker, Mar. 18, 2015, *available at* http://www.seattletimes.com/business/local-business/feds-warned-premera-about-security-flaws-before-breach/ (last visited Mar. 22, 2015).

[13] U.S. Office of Personnel Management, Office of the Inspector General, Office of Audits, Audit of Information Systems General and Application Controls at Premera Blue Cross 7 (Nov. 28, 2014), https://s3.amazonaws.com/s3.documentcloud.org/documents/1688453/opm-audit.pdf. The Final Audit Report was delivered to Premera on November 28, 2014, but the audit's initial findings were delivered to Premera in April 2014. Premera then had an opportunity to respond before the audit findings became final.

[14] *Id.*

[15] *Id.* at 8.

TERRELL MARSHALL DAUDT & WILLIE PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.350.3528
www.tmdwlaw.com

44. Ms. Connor, Ms. Cossey and Mr. Mountjoy took immediate steps to guard against identity theft. These steps include, or will imminently include, the following:

a. Filing a report of the breach with the Federal Trade Commission (FTC). The FTC report does not permit an individual to file a report on behalf of minor children;

b. Freezing credit individual credit reports with each of the three major credit reporting bureaus;

c. The major credit bureaus, however, charge $30 to freeze a credit report by default. This charge can be avoided only if the filer has previously filed a police report. To file a police report, the filer must submit the FTC report number. Upon information and belief, many members of the Class will incur charges freezing their credit report because it is not obvious that the cost is waived only where one has previously filed a police report. Premera has offered no assistance in this regard.

d. Further, upon information and belief, the three major credit reporting bureaus maintain websites that are difficult to navigate for the average user and often unclear as to what is provided as a free service and what is not a free service. Upon information and belief, many members of the Class will pay for reporting services that are not needed because they simply do not understand the process, and Premera has not offered sufficient guidance to navigate this process.

45. Each of these steps requires significant time and individual hardship. Ms. Connor has spent hours simply attempting to report the data breach on behalf of herself and her children. Moreover, it is often unclear what must be done in order to comprehensively protect oneself. Premera has offered no third-party assistance to help potential victims navigate the reporting process.



TERRELL MARSHALL DAUDT & WILLIE PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.350.3528
www.tmdwlaw.com

46. Premera has stated that it has "no evidence to date that [compromised] data has been used inappropriately."[16] Upon information and belief, however, it is likely that customer files are now on sale on the black market or will be in the near future.

47. Premera has also offered two years of free credit monitoring to affected customers. For reasons explained in more detail below, credit monitoring is entirely inadequate given the breadth of information stolen. Credit monitoring does very little to protect against tax or insurance fraud, or to prevent imposters from obtaining medical treatment or prescription drugs fraudulently. Premera offers its customers nothing to guard against these reasonably foreseeable threats.

**C. The Value of the Stolen Data**

48. The breadth of data compromised in the Premera hack is astounding and therefore is particularly valuable to thieves. The compromised data leaves Premera customers especially vulnerable to identity theft, tax fraud, medical fraud, credit and bank fraud, and more. As Pam Dixon, executive director of the World Privacy Forum, stated in response to Premera's breach: "When someone has your clinical information, your bank account information, and your Social Security number, they can commit fraud that lasts a long time. The kind of identity theft that is on the table here is qualitatively and quantitatively different than what is typically possible when you lose your credit card . . . ."[17]

49. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change.

50. The Social Security Administration has warned that identity thieves can use an individual's Social Security number and good credit score to apply for additional credit lines.

---

[16] Statement of Jeffrey Roe, *available at* http://www.premeraupdate.com/ (last visited Mar. 22, 2015).

[17] Premera Hack: What Criminals Can Do With Your Healthcare Data, Christian Science Monitor, Jaikumar Vijayan, Mar. 20, 2015, *available at* http://www.csmonitor.com/World/Passcode/2015/0320/Premera-hack-What-criminals-can-do-with-your-healthcare-data (last visited Mar. 22, 2015).



TERRELL MARSHALL DAUDT & WILLIE PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.350.3528
www.tmdwlaw.com

Such fraud may go undetected until debt collection calls commence months, or even years, later.[18]

51. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity. Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. This, in turn, may cause conflict or suspicion between an employer and employee, and may trigger investigations of the employee that require time and expense to defend. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected. It can take months or years, as well as significant expense to the victim, to correct the fraud with the IRS.

52. The incidence of fraudulent tax filings has increased dramatically over the past years. The IRS paid an estimated $5.2 billion in tax refunds obtained from identity theft in 2013, while it prevented an additional $24.2 billion in fraudulent transfers the same year.[19]

53. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

54. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to

[18] Social Security Administration, Identity Theft and Your Social Security Number, http://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Mar. 22, 2015).

[19] FBI Probes Rash of Fraudulent State Tax Returns Filed Through Turbo Tax, LA Times, Shan Li, Feb. 11, 2015, *available at* http://www.latimes.com/business/la-fi-turbotax-fbi-20150212-story.html (last visited Mar. 22, 2015).

TERRELL MARSHALL DAUDT & WILLIE PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.350.3528
www.tmdwlaw.com

link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[20]

55. Another danger, according to the publisher of *Privacy Journal*, Robert Ellis Smith, is that thieves use stolen Social Security numbers to obtain medical care in someone else's name.[21]

56. Medical identity fraud affected 2.3 million people in 2014—an increase of 21% over the previous year. A study by the Ponemon Institute concluded that victims of such fraud spend an average of $13,500 to resolve problems stemming from medical identity theft.[22]

57. Moreover, fraudulent medical treatment can have non-financial impacts as well. Deborah Peel, executive director of Patient Privacy Rights, has described scenarios in which an individual may be given an improper blood type or administered medicines because his or her medical records contain information supplied by an individual obtaining treatment under a false name.[23]

58. In the Premera hack, customer clinical information was compromised. This means any information contained in an individual's medical records is subject to disclosure or, worse, medical blackmail.

59. The Ponemon Institute study concluded that a victim of medical identity theft typically does not learn of the fraudulent treatment for three months. To guard against medical identity fraud, cyber security experts suggest that individuals routinely obtain the most recent copy of their medical records and inspect them for discrepancies. Premera's proposed customer

---

[20] Victims of Social Security Number Theft Find It's Hard to Bounce Back, NPR, Brian Naylor, Feb. 9, 2015, *available at* http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited Mar. 22, 2015).

[21] Victims of Social Security Number Theft Find It's Hard to Bounce Back, NPR, Brian Naylor, Feb. 9, 2015, *available at* http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited Mar. 22, 2015).

[22] Ponemon Institute LLC, Fifth Annual Study on Medical Identity Theft 2 (Feb. 2015), *available at* http://assets.fiercemarkets.com/public/healthit/ponemonmedidtheft2015.pdf (last visited Mar. 23, 2015).

[23] *See* 2015 is Already the Year of the Health-Care Hack—and It's Only Going to Get Worse, Wash. Post, Andrea Peterson, Mar. 20, *available at* http://www.washingtonpost.com/blogs/the-switch/wp/2015/03/20/2015-is-already-the-year-of-the-health-care-hack-and-its-only-going-to-get-worse/ (last visited Mar. 22, 2015).



TERRELL MARSHALL DAUDT & WILLIE PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.350.3528
www.tmdwlaw.com

solutions do nothing to address the problem of medical identity theft, and Premera has done nothing to advise its customers how to obtain and inspect their medical records for fraud to comport with best practices identified by security experts.

60. The victims of the Premera breach are also now at heightened risk of health insurance discrimination. Stolen medical and clinical information may be improperly disclosed for use to discriminate in the provision of healthcare to insureds and prospective insureds. Individuals risk denial of coverage, improper "redlining," and denial or difficulty obtaining disability or employment benefits because information was improperly disclosed to a provider. This risk is pervasive and widespread. Indeed, most states maintain government agencies that investigate and combat health insurance discrimination, as does the Office for Civil Rights in the Department of Health and Human Services.

61. The danger of identity theft is compounded when a minor's Social Security number and personal information is compromised. Whereas adults can periodically monitor their own credit reports, minors typically have no credit to monitor. Thus, it can be difficult to safeguard against fraud. Thieves who steal a minor's identity may use it for years before the crime is discovered.

62. Premera is offering a "family secure service" through Experian for customers with minor children. This service provides monthly monitoring to ascertain whether a minor's Social Security number has been used to access credit. This service, while a step in the right direction, is nonetheless inadequate; it permits fraudsters a thirty-day window in which to commit fraud without fear of detection via monitoring.

63. The personal information compromised in the Premera breach is significantly more valuable than the credit card information that was compromised in the large retailer data breaches at Target and Home Depot. Victims affected by the retailer breaches could avoid much of the potential for future harm by cancelling credit or debit cards and obtaining



TERRELL MARSHALL DAUDT & WILLIE PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.350.3528
www.tmdwlaw.com

replacements. The information compromised in the Premera breach is difficult, if not impossible, to change—Social Security number, name, date of birth, clinical information, etc.

64. These data, as one would expect, demand a much higher price on the black market. Martin Walter, senior director at cyber security firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[24]

65. This estimate may be low. A recent PriceWaterhouseCoopers report stated that an identity theft kit containing health insurance credentials can be worth up to $1,000 on the black market, while stolen credit cards may go for $1 each.

66. Premera has announced that it will offer free credit monitoring services for two years. As security blogger Brian Krebs has explained, however, "the sad truth is that most services offer little in the way of real preventative protection against the fastest-growing crime in America [identity theft]."[25] Credit monitoring services, in other words, may inform individuals of fraud after the fact, but do little to thwart fraud from occurring in the first instance. Moreover, these services do very little to defend against medical identity theft or misuse of Social Security numbers for non-financial fraud.

67. The implications of the Premera data breach are indeed serious. But these implications were known *ex ante*. Premera should have—and could have—done more to fulfill its duty to safeguard the data with which its customers entrusted it. And it could—and should—do more to protect its customers now that a breach has occurred.

[24] Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers, IT World, Tim Greene, Feb. 6, 2015, *available at* http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Mar. 22, 2015).

[25] Brian Krebs, Are Credit Monitoring Services Worth It?, Krebs on Security, Mar. 4, 2014, http://krebsonsecurity.com/2014/03/are-credit-monitoring-services-worth-it/ (last visited Mar. 22, 2015).

TERRELL MARSHALL DAUDT & WILLIE PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.350.3528
www.tmdwlaw.com

**D. The Healthcare and Health Insurance Industry—Including Premera—is on Notice that it is a Target of Cyber Thieves**

68. Healthcare and health insurance companies, including Premera, are well aware that they are the target of cyber thieves, yet the industry has failed to implement the cyber security reforms implemented across other industries.

69. Martin Walter, senior director at RedSeal, has stated that companies in the healthcare industry "in comparison spend significantly less on security, making them tentatively easier targets."[26] Cyber security analysts generally believe that the healthcare industry lags far behind other industries when it comes to cyber security.[27]

70. Dave Kennedy, chief executive of information security firm TrustedSEC, has explained that healthcare organizations are targets because they maintain troves of data with significant resale value in black markets and their security practices are less sophisticated than other industries. "Health organizations sometimes rely on legacy systems, and some have not invested in cybersecurity at a rate that matches the urgency of the threats they face. The medical industry is years behind other industries when it comes to security."[28]

71. The cybersecurity firm WhiteHat recently reported that in the healthcare industry, only 24% of known security flaws are fixed at any given time.[29] Indeed, the Office of Personnel Management's audit of Premera suggests the applicability of this statistic to the instant case. That audit identified, *inter alia*, vulnerabilities related to Premera's failure to implement critical security patches and software updates, and warned that "[f]ailure to

---

[26] Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers, IT World, Tim Greene, Feb. 6, 2015, *available at* http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Mar. 22, 2015).

[27] *See* Data Breach at Anthem May Forecast a Trend, New York Times, Reed Abelson & Julie Creswell, Feb. 6, 2015, *available at* http://www.nytimes.com/2015/02/07/business/data-breach-at-anthem-may-lead-to-others.html (last visited Mar. 22, 2015).

[28] *See* 2015 is Already the Year of the Health-Care Hack—and It's Only Going to Get Worse, Wash. Post, Andrea Peterson, Mar. 20, *available at* http://www.washingtonpost.com/blogs/the-switch/wp/2015/03/20/2015-is-already-the-year-of-the-health-care-hack-and-its-only-going-to-get-worse/ (last visited Mar. 22, 2015).

[29] Premera Hack: What Criminals Can Do With Your Healthcare Data, Christian Science Monitor, Jaikumar Vijayan, Mar. 20, 2015, *available at* http://www.csmonitor.com/World/Passcode/2015/0320/Premera-hack-What-criminals-can-do-with-your-healthcare-data (last visited Mar. 22, 2015).



TERRELL MARSHALL DAUDT & WILLIE PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.350.3528
www.tmdwlaw.com

promptly install important updates increases the risk that vulnerabilities will not be remediated and sensitive data could be breached."

72. If the Office of Personnel Management audit were not enough, the events of 2014 alone should have placed Premera on notice of the need to improve its cyber security systems. In August 2014, Community Health Systems, the second largest for-profit hospital chain in the United States, was hacked and the Social Security numbers of 4.5 million customers were stolen. This prompted a "flash warning" by the FBI to entities in the healthcare industry that it had observed "malicious actors targeting health care related systems, perhaps for the purpose of obtaining Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."[30]

73. Earlier in the year, over 12,000 patients' records were compromised when hackers gained access to the accounts of employees of Centura Health Systems of Colorado Springs. This event was preceded by a breach at Texas's St. Joseph Health System compromising 405,000 patient records. In spite of these industry warnings, Premera took insufficient steps to ensure its IT systems had not been breached until January 2015—nearly nine months after hackers gained access to its system.

74. The history of cyber security breaches in the industry, and the warnings that are now all but ubiquitous, have placed companies operating in the industry on notice of the duty to safeguard customers' personal and health information. If anything, this history of failure should spur greater efforts to implement top-of-the-line cyber security measures that exceed the industry standard. Indeed, customers expect that healthcare companies will take every precaution to safeguard their personal information. The unfortunate reality, as Les Funtleyder, a health care portfolio manager, observed, is that "health care has been very slow to adopt

[30] FBI Warns Healthcare Firms They Are Targeted By Hackers, Reuters, Aug. 20, 2014, *available at* http://www.reuters.com/article/2014/08/20/us-cybersecurity-healthcare-fbi-idUSKBN0GK24U20140820 (last visited Mar. 22, 2015).

TERRELL MARSHALL DAUDT & WILLIE PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.350.3528
www.tmdwlaw.com

almost every technological advance. Right now, a lot of health care companies are sitting ducks."[31]

## V. CLASS ACTION ALLEGATIONS

75. Plaintiffs bring this lawsuit as a class action on their own behalf and on behalf of all other persons similarly situated as members of the proposed Class pursuant to Federal Rules of Civil Procedure 23(a) and (b)(3) and/or (b)(2). This action satisfies the numerosity, commonality, typicality, adequacy, predominance, and superiority requirements of those provisions.

76. The proposed nationwide class is defined as:

> Nationwide Class
>
> All persons in the United States who were insured by Premera and/or its affiliates for any period of time beginning in 2002 until January 29, 2015, and all persons in the United States who were not Premera insureds but who are or were Blue Cross Blue Shield customers and who received medical treatment in Washington or Alaska between 2002 and January 29, 2015.

77. Plaintiff also bring this action on behalf of a Washington State Class, defined as:

> Washington Class
>
> All persons who reside in Washington and who were insured by Premera and/or its affiliates for any period of time beginning in 2002 until January 29, 2015.

78. Plaintiffs also bring this action on behalf of a Premera Treatment Subclass, defined as:

> Premera Treatment Subclass
>
> All persons who were not insured by Premera and/or its affiliates for any period of time beginning in 2002 until January 29, 2015, but who were insured by Blue Cross Blue Shield and received

[31] Indianapolis Business Journal, *Anthem's IT System Had Cracks Before Hack*, J.K. Wall, Feb. 14, 2015, http://www.ibj.com/articles/51789-anthems-it-system-had-cracks-before-hack (last visited Mar. 22, 2015).



TERRELL MARSHALL DAUDT & WILLIE PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.350.3528
www.tmdwlaw.com

> medical treatment in Washington or Alaska between 2002 and January 29, 2015.

Excluded from the Classes and Subclass are: (1) Defendant, any entity or division in which Defendant has a controlling interest, and its legal representatives, officers, directors, assigns, and successors; (2) the Judge to whom this case is assigned and the Judge's staff; and (3) governmental entities. Plaintiffs reserve the right to amend the Class definition if discovery and further investigation reveal that the Class should be expanded, divided into subclasses or modified in any other way.

**A. Numerosity and Ascertainability**

79. Although the exact number of class members is uncertain and can be ascertained only through appropriate discovery, the number is great enough such that joinder is impracticable. The disposition of the claims of these class members in a single action will provide substantial benefits to all parties and to the Court. Class members are readily identifiable from information and records in Premera's possession, custody, or control.

**B. Typicality**

80. Plaintiffs' claims are typical of the claims of the Class in that Plaintiffs, like all class members, entrusted personal and health information to Premera in connection with healthcare services or treatment. Plaintiffs, like all class members, have been damaged by Premera's conduct in that their personal and health information, including their Social Security number and clinical information, have been compromised by Premera's failure to fulfill its duties under the law. Further, the factual bases of Premera's misconduct are common to all class members and represent a common thread of misconduct resulting in injury to all class members.

**C. Adequate Representation**

81. Plaintiffs will fairly and adequately represent and protect the interests of the Class. Plaintiffs have retained counsel with substantial experience in prosecuting consumer and data breach class actions, and therefore Plaintiffs' counsel is also adequate under Rule 23.

TERRELL MARSHALL DAUDT & WILLIE PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.350.3528
www.tmdwlaw.com

82. Plaintiffs and their counsel are committed to vigorously prosecuting this action on behalf of the Class and have the financial resources to do so. Neither Plaintiffs nor her counsel has interests adverse to those of the Class.

**D. Predominance of Common Issues**

83. There are numerous questions of law and fact common to Plaintiffs and the class members that predominate over any question affecting only individual class members. The answers to these common questions will advance resolution of the litigation as to all class members. These common legal and factual issues include:

a. Whether Premera owed a duty to Plaintiffs and members of the Class to take reasonable measures to safeguard their personal information;

b. Whether Premera knew or should have known that its cyber security systems were vulnerable to attack;

c. Whether Premera's breach of a legal duty caused its cyber security systems to be compromised, resulting in the loss and/or potential loss of 11 million member files;

d. Whether Premera owed a duty to Plaintiffs and members of the Class to provide timely and adequate notice of the Premera data breach and the risks posed thereby, and whether Premera's notice was, in fact, timely;

e. Whether Premera violated Washington state law requiring notice within the "most expedient time possible" when a data breach occurs; and

f. Whether Plaintiffs and class members are entitled to recover actual damages, statutory damages, and/or punitive damages.

**E. Superiority**

84. Plaintiffs and class members have all suffered and will continue to suffer harm and damages as a result of Premera's unlawful and wrongful conduct. A class action is superior to other available methods for the fair and efficient adjudication of this controversy.

TERRELL MARSHALL DAUDT & WILLIE PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.350.3528
www.tmdwlaw.com

85. Absent a class action, most class members would likely find the cost of litigating their claims prohibitively high and would therefore have no effective remedy at law. Further, without class litigation, class members will continue to incur damages and Premera is likely to repeat its misconduct.

86. Class treatment of common questions of law and fact is also a superior method to multiple individual actions or piecemeal litigation in that class treatment will conserve the resources of the courts and the litigants, and will promote consistency and efficiency of adjudication.

## CAUSES OF ACTION

### VI. FIRST CLAIM FOR RELIEF
### Negligence
### (Asserted on Behalf of the Nationwide Class)

87. Plaintiffs hereby incorporate by reference the allegations contained in the preceding paragraphs of this Complaint.

88. Plaintiffs bring this Claim on behalf of the Nationwide Class under Washington law.

89. In the alternative, Plaintiffs bring this Claim on behalf of the Washington Class under Washington state law.

90. Premera required Plaintiffs and class members to submit non-public personal and health information in order to acquire coverage under a health insurance policy and/or receive treatment in the Blue Cross Blue Shield network while in Washington or Alaska. Premera collected and stored this data. It therefore assumed a duty of care to use reasonable means to secure and safeguard this personal and health information, to prevent disclosure of the information, and to guard the information from theft. Premera's duty included a responsibility to implement a process by which it could detect a breach of its security systems in a reasonably expeditious period of time.



TERRELL MARSHALL DAUDT & WILLIE PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.350.3528
www.tmdwlaw.com

91. Premera's duty arises from the common law, as well as the principles embodied in Washington state law, as set forth herein, Article I, Section 7 of the Washington Constitution, and HIPAA.

92. Premera breached its duty of care by failing to secure and safeguard the personal and health information of Plaintiffs and the Class. Premera negligently maintained systems that it knew were vulnerable to a security breach. It was made aware of these vulnerabilities, yet failed to rectify them. Further, Premera negligently stored financial and health information unencrypted on the same database, making it more likely a breach would net a greater (and more dangerous) breadth of personal information.

93. Given the risks associated with data theft, Premera also assumed a duty of care to promptly and fully notify and inform its customers should their personal information be compromised and/or stolen.

94. Premera breached this duty of care when it unreasonably waited over six weeks to notify the Class that its security systems had been breached. Premera learned of the breach on January 29, 2015, yet said nothing to notify those affected for over six weeks. Premera even went so far as to assure its customers that they had nothing to fear, emphasizing that the breach at Anthem Inc. in early February 2015 did not affect Premera customers. While this is true, Premera offered these assurances knowing full well that its customers' data was compromised by an independent breach that potentially affected an even greater breadth of information than the breach experienced at Anthem Inc. Premera continues to breach this duty of care, by failing to share crucial information with Plaintiffs and the Class.

95. Plaintiffs and the Class have suffered harm as a result of Premera's breach. The personal and health information of Plaintiffs and the Class have been exposed, subjecting each member of the Class to identity theft, credit and bank fraud, Social Security fraud, tax fraud, medical identity fraud, and myriad other varieties of identity fraud.



TERRELL MARSHALL DAUDT & WILLIE PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.350.3528
www.tmdwlaw.com

96. Plaintiffs and the Class have suffered monetary damages and will continue to be injured and incur damages in the future both in an effort to protect themselves and to remedy acts of fraudulent activity. Plaintiffs and the Class have suffered and/or are reasonably likely to suffer theft of personal and health information; costs associated with prevention, detection, and mitigation of identity theft and/or fraud; costs associated with time spent and productivity loss resulting from addressing the consequences of fraud in any of its myriad forms; and damages from the unconsented exposure of personal and health information due to this breach.

## VII. SECOND CLAIM FOR RELIEF
### Negligence Per Se
### (Asserted on Behalf of the Nationwide Class)

97. Plaintiffs hereby incorporate by reference the allegations contained in the preceding paragraphs of this Complaint.

98. Plaintiffs bring this Claim on behalf of the Nationwide Class under Washington law.

99. In the alternative, Plaintiffs bring this Claims on behalf of the Washington Class.

100. Under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Premera had a duty to secure and safeguard the personal information of its customers. Premera acknowledged this duty to its customers in its Notice of Privacy Practices, and warranted that it would comport with its duties under HIPAA.

101. Premera violated HIPAA by failing to secure and safeguard the personal information entrusted to it by Plaintiffs and the Class. Further, Premera failed to implement protections against "reasonably anticipated threats," 45 C.F.R. § 164.306, and failed to encrypt customer data or implement an equivalent alternative measure and document the reason or reasons that encryption was not reasonable, *id.* § 164.312.

102. Premera's failure to comply with HIPAA and regulations promulgated thereto constitutes negligence per se.

TERRELL MARSHALL DAUDT & WILLIE PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.350.3528
www.tmdwlaw.com

103. As a result of Premera's negligence per se, Plaintiffs and the Class have suffered monetary damages and will continue to be injured and incur damages in the future both in an effort to protect themselves and to remedy acts of fraudulent activity. Plaintiffs and the Class have suffered and/or are reasonably likely to suffer theft of personal and health information; costs associated with prevention, detection, and mitigation of identity theft and/or fraud; costs associated with time spent and productivity loss resulting from addressing the consequences of fraud in any of its myriad forms; and damages from the unconsented exposure of personal and health information due to this breach.

## VIII. THIRD CLAIM FOR RELIEF
### Bailment
### (Asserted on Behalf of the Nationwide Class)

104. Plaintiffs hereby incorporate by reference the allegations contained in the preceding paragraphs of this Complaint.

105. Plaintiffs bring this Claim on behalf of the Nationwide Class under Washington law.

106. In the alternative, Plaintiffs bring this Claim on behalf of the Washington State Class under Washington law.

107. Plaintiffs and the Class delivered personal and health information to Premera for the exclusive purpose of obtaining health insurance and/or medical treatment.

108. By delivering their personal and health information to Premera, Plaintiffs and the Class intended and understood that Premera would adequately safeguard their personal and health information from being accessed by or disclosed to unauthorized persons.

109. Premera accepted possession of the personal and health information of Plaintiffs and the Class for the purpose of providing health insurance to Plaintiffs and the Class.

110. By accepting possession of the personal and health information of Plaintiffs and the Class, Premera understood that Plaintiffs and the Class expected Premera to adequately



TERRELL MARSHALL DAUDT & WILLIE PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.350.3528
www.tmdwlaw.com

safeguard their information. Accordingly, a bailment (or deposit) was established for the mutual benefit of the parties.

111. During the bailment, Premera owed a duty to Plaintiffs and the Class to exercise reasonable care, diligence, and prudence in protecting their personal and health information.

112. Premera breached its bailment and its duty of care by failing to take appropriate measures to safeguard and protect the personal and health information of Plaintiffs and the Class. This breach resulted in the unlawful and unauthorized access to and misuse of the personal and health information of Plaintiffs and the Class.

113. Premera further breached its bailment and its duty to safeguard the personal and health information of Plaintiffs and the Class by failing to timely and completely notify Plaintiffs and the Class that their private information was compromised as a result of the breach.

## IX. FOURTH CLAIM FOR RELIEF
### Breach of Contract
### (Asserted on Behalf of the Washington State Class and the Premera Treatment Subclass)

114. Plaintiffs hereby incorporate by reference the allegations contained in the preceding paragraphs of this Complaint.

115. Plaintiffs bring this Claim on behalf of the Washington State Class under Washington law and the Premera Treatment Subclass under Washington law.

116. Premera entered into written contracts with Plaintiffs and the Class in which it agreed to provide a health insurance policy for a fixed period of time in exchange for periodic premium payments.

117. As part of its contractual agreement, Premera undertook the obligation to maintain the security of its customers' personal and health information. Premera recognizes this obligation in its Notice of Privacy Practices, where it states that "it must take measures to protect the privacy of your personal information" under both HIPAA and the Gramm-Leach-Bailey Act.



TERRELL MARSHALL DAUDT & WILLIE PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.350.3528
www.tmdwlaw.com

118. Premera breached its contractual obligation by failing to safeguard the personal and health information of Plaintiffs and the Class, and by failing to timely notify Plaintiffs and the Class that their personal and health information was compromised by a data breach.

119. In addition, Premera entered into a contract with members of the Premera Treatment Subclass when it provided each subclass member a Notice of Privacy Practices in connection with medical treatment in Washington or Alaska. By providing this Notice to subclass members, Premera undertook the obligation to maintain the security of subclass members' personal and health information. In the alternative, and if the Court finds that Premera did not enter into an explicit contract with the Premera Treatment Subclass, then Plaintiffs ask that the Court find that Premera entered into an implied contract with the Subclass, and that Premera violated this implied contract by failing to abide by its privacy warranties.

120. Plaintiffs and the Washington State Class, as well as the Premera Treatment Subclass, seek actual damages as described herein to be proven at trial, as well as attorneys' fees and costs as permitted by law.

## X. FIFTH CLAIM FOR RELIEF
## Violation of Breach of Fiduciary Duty
## (Asserted on Behalf of the Nationwide Class)

121. Plaintiffs hereby incorporate by reference the allegations contained in the preceding paragraphs of this Complaint.

122. Plaintiffs bring this Claim on behalf of the Nationwide Class under Washington law.

123. Premera collected and stored highly personal and private information, including health information, belonging to Plaintiffs and members of the Class. Because this information is of a heightened sensitivity and importance, it receives special protection under federal law. Indeed, HIPAA protects all "individually identifiable health information," as well as individual identifiers such as Social Security numbers and medical identification numbers. *See, e.g.*, 45



TERRELL MARSHALL DAUDT & WILLIE PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.350.3528
www.tmdwlaw.com

C.F.R. § 160.103. What is more, HIPAA imposes heightened duties on entities like Premera that collect and store such information, subjecting them to a range of penalties when protected health information is wrongfully disclosed. *See, e.g.*, 42 U.S.C. §§ 1320d-5, 1320d-6.

124. The protected health information also receives heightened protection under Washington state law. As explained below, the Revised Code of Washington applies special duties upon a business that stores "personal information," including Social Security numbers, credit and banking information. *See* RCW 19.255.010. Where a business suffers a data breach exposing such information, the law places heightened duties of disclosure on that business. *Id.*

125. By virtue of its collection of highly personal information, including health information, and the warranties made in its Notice of Privacy Practices, a fiduciary relationship arose between Premera and the class members that is actionable at law.

126. By virtue of this fiduciary relationship, Premera owed Plaintiffs and members of the Class a fiduciary duty to safeguard the personal and health information that it collected and stored; to warn Plaintiffs and the Class when it learned that the security of the collected data may be vulnerable; and to immediately and fully notify Plaintiffs and the Class when it knew that its cyber security systems had been breached. This duty required Premera to ensure that the interests of Plaintiffs and the Class would be adequately cared for, both before and after the security breach. By virtue of its duty, Premera owes Plaintiffs and the Class assistance in protecting themselves now that a breach has occurred, not just from financial fraud, but also from medical identity fraud, health insurance discrimination, tax fraud, and other forms of identity fraud described herein.

127. In the event that the Court finds that this Claim may not be raised on behalf of the Nationwide Class, Plaintiffs and the Class bring this Claim on behalf of the Washington State Class under Washington law and, separately, on behalf of the Premera Treatment Subclass under the law of class members' respective domicile.



TERRELL MARSHALL DAUDT & WILLIE PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.350.3528
www.tmdwlaw.com

128. As a result of Premera's breach of its fiduciary duties, Plaintiffs and the Class have suffered actual damages, and prospective damages that are reasonably likely to arise. Premera has taken insufficient steps to protect the Class from these reasonably likely prospective damages, and Plaintiffs and the Class therefore also request equitable and/or injunctive relief to require Premera to take steps to prevent the forms of identity fraud alleged herein.

## XI. SIXTH CLAIM FOR RELIEF
### Violation of Washington's Data Disclosure Law, RCW 19.255.010
### (Asserted on Behalf of the Washington State Class)

129. Plaintiffs hereby incorporate by reference the allegations contained in the preceding paragraphs of this Complaint.

130. Plaintiffs bring this Claim on behalf of the Washington State Class under Washington law.

131. RCW 19.255.010 states that any business that conducts business in the state and that "maintains computerized data that includes personal information" shall disclose "any breach of the security of the data immediately following discovery" of that breach. A business must disclose the fact of the breach to any Washington resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

132. A disclosure must occur "in the most expedient time possible and without unreasonable delay."

133. Premera experienced a "breach of the security system" as that phrase is used in this Section.

134. Premera maintained unencrypted "computerized data" that included "personal information," as those phrases are used in this Section.

135. Premera failed to disclose the fact of the breach of its security system in the most expedient time possible.



TERRELL MARSHALL DAUDT & WILLIE PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.350.3528
www.tmdwlaw.com

136. Premera's failure to provide notice in the most expedient time possible is a violation RCW 19.255.010, and also constitutes negligence per se.

137. Plaintiffs and the Washington State Class seek damages as permitted by law, as well as injunctive relief. To this day, Premera has not provided notice to the Class consistent with this Section and it should be compelled to do so without delay.

## XII. SEVENTH CLAIM FOR RELIEF
### Violation of the Washington Consumer Protection Act, RCW 19.86 *et seq.*
### (Asserted on Behalf of the Washington State Class)

138. Plaintiffs hereby incorporate by reference the allegations contained in the preceding paragraphs of this Complaint.

139. Premera is a "person" within the meaning of the Washington Consumer Protection Act, RCW 19.86.010(1), and conducts "trade" and "commerce" within the meaning of the Washington Consumer Protection Act, RCW 19.86.010(2).

140. Plaintiffs and other Class members are "persons" within the meaning of the Washington Consumer Protection Act, RCW 19.86.010(1).

141. Premera's failure to safeguard Plaintiffs' and Class members' private and financial data constitutes an unfair act because these acts or practices offend public policy as it has been established by statutes, regulations, the common law or otherwise, including, but not limited to, the public policy established by RCW 19.255.010 *et seq*.

142. Premera's failure to safeguard Plaintiffs' and Class members' private and financial data is unfair because this act or practice (1) causes substantial injury to Plaintiffs and Class members; (2) is not outweighed by any countervailing benefits to consumers or competitors; and (3) is not reasonably avoidable by consumers.

143. Premera's failure to safeguard Plaintiffs' and Class members' private and financial data is unfair because this act or practice is immoral, unethical, oppressive and/or unscrupulous.



TERRELL MARSHALL DAUDT & WILLIE PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.350.3528
www.tmdwlaw.com

144. Premera's failure to promptly notify Plaintiffs and class members of the loss of their data is unfair because these acts or practices offend public policy as it has been established by statutes, regulations, common law or otherwise, including, but not limited to, the public policy established by RCW 19.255.010 *et seq*.

145. Premera's failure to promptly notify Plaintiffs and Class members of the loss of their data is unfair because this act or practice (1) causes substantial injury to Plaintiffs and Class members; (2) is not outweighed by any countervailing benefits to consumers or competitors; and (3) is not reasonably avoidable by consumers.

146. Premera's failure to promptly notify Plaintiffs and Class members of the loss of their data is unfair because this act or practice is immoral, unethical, oppressive and/or unscrupulous.

147. Premera's unfair acts or practices have occurred in its trade or business and were and are capable of injuring a substantial portion of the public. As such, Premera's general course of conduct as alleged herein is injurious to the public interest, and the acts complained of herein are ongoing and/or have a substantial likelihood of being repeated.

148. As a direct and proximate result of Premera's unfair acts or practices, Plaintiffs and Class members suffered injury in fact.

149. Plaintiffs and the Class are therefore entitled to an order enjoining the conduct complained of herein and ordering Premera to take remedial measures to prevent similar data breaches from occurring in the future; actual damages; treble damages pursuant to RCW 19.86.090; costs of suit, including a reasonable attorney's fee; and such further relief as the Court may deem proper.

## XIII. PRAYER FOR RELIEF

Plaintiffs, on behalf of themselves and all others similarly situated, request the Court to enter judgment against Defendant, as follows:



TERRELL MARSHALL DAUDT & WILLIE PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.350.3528
www.tmdwlaw.com

A. An order certifying the proposed Class designating Plaintiffs as the named representatives of the Class, and designating the undersigned as Class Counsel;

B. An order awarding Plaintiffs and the Class relief, including actual and statutory damages, as well as equitable and/or injunctive relief as requested herein;

C. An injunction ordering Premera to immediately notify each individual whose personal information was compromised and/or an order awarding Plaintiffs and the Class preliminary or other equitable or declaratory relief as may be appropriate by way of applicable state or federal law and as requested herein;

D. Any additional orders or judgments as may be necessary to prevent further unlawful practices and to restore to any person in interest any money or property that may have been acquired by means of the violations;

E. An award of attorneys' fees and costs, as provided by law;

F. An award of pre-judgment and post-judgment interest, as provided by law;

G. Leave to amend this Complaint to conform to the evidence produced at trial; and

H. Any other favorable relief as may be available and appropriate under law or at equity.

## XIV. JURY DEMAND

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiffs demand a trial by jury of any and all issues in this action so triable of right.

RESPECTFULLY SUBMITTED AND DATED this 26th day of March, 2015.

TERRELL MARSHALL DAUDT & WILLIE PLLC

By: /s/ Beth E. Terrell, WSBA #26759

Beth E. Terrell, WSBA #26759
Email: bterrell@tmdwlaw.com
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
Telephone: (206) 816-6603
Facsimile: (206) 350-3528



TERRELL MARSHALL DAUDT & WILLIE PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.350.3528
www.tmdwlaw.com

John A. Yanchunis
Email: jyanchunis@ForThePeople.com
MORGAN & MORGAN
201 North Franklin Street, 7th Floor
Tampa, Florida 33602
Telephone: (813) 223-5505
Facsimile: (813) 223-5402

Robin L. Greenwald
Email: rgreenwald@weitzlux.com
James J. Bilsborrow
Email: jbilsborrow@weitzlux.com
WEITZ & LUXENBERG, P.C.
700 Broadway
New York, New York 10003
Telephone: (212) 558-5500
Facsimile: (646) 293-7937

Steven W. Teppler
Email: steppler@abbottlawpa.com
F. Catfish Abbott
Email: fabbott@abottlawpa.com
ABBOTT LAW GROUP P.A.
2929 Plummer Cove Road
Jacksonville, Florida 32223
Telephone: (904) 292.1111
Facsimile: (904) 292-1200

Joel R. Rhine
Email: jrr@rhinelawfirm.com
RHINE LAW FIRM, P.C.
1612 Military Cutoff Road, Suite 300
Wilmington, North Carolina 28403
Telephone: (910) 772-9960
Facsimile: (910) 772-9062

*Attorneys for Plaintiffs*